



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/831,046	05/03/2001	Martin Euchner	P01,0142	8224
24131	7590	05/27/2005	EXAMINER	
LERNER AND GREENBERG, PA P O BOX 2480 HOLLYWOOD, FL 33022-2480			DINH, MINH	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 05/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/831,046

Applicant(s)

EUCHNER, MARTIN

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 12 November 2004.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 2-7 and 11-18 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 2-7, 11-15, 17 and 18 is/are rejected.  
7) ☒ Claim(s) 16 is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 03 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is in response to the amendment filed 11/12/2004. Claims 2-7 have been amended; claims 1 and 8-10 have been cancelled; claims 11-18 have been added. The specification has also been amended.

### ***Response to Arguments***

2. Applicant's arguments with respect to claim 11 have been considered but are not persuasive. Applicant's amendments have necessitated a new search and new grounds of rejection.

### ***Oath/Declaration***

3. A substitute declaration was filed on 12/20/2004. The substitute declaration is defective because the specification to which the declaration is directed has not been adequately identified (i.e., the box indicating that the previously-filed specification has not been checked). See MPEP § 602.

### ***Claim Objections***

4. Claim 12 is objected to because of the following informalities: it depends on claim 1 which has been cancelled. For examination purpose, claim 12 is interpreted as being depended upon claim 11. Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 7 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 7 recites the limitation "wherein data transmitted is confidential data" in lines 2-3. However, claim 7 depends on claim 1 in which data is also transmitted in plaintext (see clause c). It is not clear why confidential data is transmitted in plaintext which everyone, whether authorized or not, has access to. For examination purpose, the limitation is interpreted as "wherein unauthorized modification to data transmitted can be detected".

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 2-7, 11-15 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier ("Applied Cryptography") in view of Menezes et al ("Handbook of Applied Cryptography").

Regarding claims 11-12, 6-7, 17-18, Schneier discloses a method for encrypted key exchange with Diffie-Hellman which is a public-key algorithm. Specifically, Schneier

discloses that Alice performs an exponential operation using prescribed known values  $g$  and  $n$  and her random number  $r_A$  to obtain her exponential value  $g^{r_A} \bmod n$ . Alice then sends Bob a message comprising her identification and her exponential value (p. 519, Implementing EKE with Diffie-Hellman). Schneier further discloses that Alice and Bob share a symmetric key  $P$ . However, Schneier does not disclose that Alice encodes her message with  $P$  to obtain an encoded message and sends Bob the encoded message together with the message as a composite message and that Bob authenticates Alice only using the composite message. Menezes discloses using MAC to provide data integrity and message authentication. Specifically, Menezes discloses that a sender encodes a message to be sent with a symmetric key shared between the sender and a receiver to generate a MAC (Message Authentication Code) for the message, sends a composite message including the message and the MAC to the receiver who authenticates the sender using only the composite message (Section 9.6.1 Background and definitions, p. 359-362; Section 9.6.3 Data integrity using a MAC alone, p. 364). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method such that Alice encodes her message with a shared key to obtain an encoded message and sends Bob the encoded message together with the message as a composite message and that Bob authenticates Alice only using the composite message, as taught by Menezes. The motivation for doing so would have been that the receiver could determine that data transmitted is authentic and has integrity.

Regarding claims 2-3, Schneier further discloses that the exponential operation is a Diffie-Hellman function, which is based on discrete logarithms in a finite cyclic group, the finite cyclic group being a multiplicative group of the integers modulo of a prescribed prime number (p. 513-514, Diffie-Hellman).

Regarding claims 13-14 and 4-5, Schneier further discloses that the result of the exponential operation is used as a second key which is determined in relation to  $g^{r_A r_B} \bmod n$  by virtue of the fact that Bob performs an exponential operation using  $g$  and  $n$  and his random number  $r_B$  to obtain his exponential value  $g^{r_B} \bmod n$ , which is encoded with key  $P$  and transmitted to Alice in a message (p. 520, Implementing EKE with Diffie-Hellman). Schneier further discloses that the second key is a session key or an authorization to a service on the second entity (p. 521, Applications of EKE).

Regarding claim 15, Schneier does not disclose the message transmitted to Alice comprises a time stamp in plaintext. Menezes discloses utilizing a time stamp in plaintext and encoded form in a transmitted message (p. 362, Transaction authentication). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method such that the message transmitted to Alice comprises a time stamp in plaintext and encoded form, as taught by Menezes. The motivation for doing so would have been to prevent undetectable message replay.

***Allowable Subject Matter***

9. Claim 16 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter. Regarding claim 16, the limitations "the encoding is performed with the first key utilizing a symmetric encoding method", in combination with elements of the parent claim, have not been taught by prior art.

***Conclusion***

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 4,200,770 to Hellman et al.

U.S. Patent No. 5,241,599 to Bellovin et al.

U.S. Patent No. 5,491,749 to Rogaway

U.S. Patent No. 6,226,383 to Jablon

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2132

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).




Application/Control Number: 09/831,046  
Art Unit: 2132

Page 8

MD

Minh Dinh  
Examiner  
Art Unit 2132

5/20/05

  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100